REMARKS

This paper is responsive to a *non-final* Office action dated May 27, 2008. Claims 3-23 were examined and rejected. All rejections are traversed.

Preliminaries and Informalities

Applicant appreciates the withdrawal of each of the rejections made in the prior Official action, including those based on U.S. Patent No. 7,051,204 to Pitsos (hereinafter "*Pitsos*"). Unfortunately, it appears that, like the *Pitsos*-based rejections before, disclosure attributed by the Office to the newly applied reference, US Patent Application Publication 2005/0021969 naming Williams et al. as inventors (hereinafter "*Williams*"), is simply not consistent with the actual disclosure thereof. In particular, and as before, the Office appears to mistake use of routine PKI terminology for a *prima facie* case of obviousness.

Claims 9 and 23 have been corrected as required by the Examiner.

Claim Rejections – 35 USC § 103, Zhao in view of Williams

Claims 3-23 stand rejected under 35 USC § 103(a) as being unpatentable over US 7,124,295 to Zhao et al. (hereinafter "*Zhao*") in view of *Williams*. In framing the rejection of independent claim 3, the Office relies on *Zhao* for disclosure of an update to a local certificate revocation list (CRL) state by application of a delta CRL to produce a resultant local CRL state. Unfortunately, the Office then goes on to attribute to a proposed combination of *Zhao* and *Williams*, disclosure that simply does not appear in either reference. In particular, while the Office properly acknowledges that *Zhao* does ***not*** disclose (i) receiving such a first hash value computed as a function of a resultant state CRL(t+n) computable by applying the delta CRL to the CRL(t) state, (ii) computing a second hash value as a function of a resultant local CRL state or (iii) comparing such second and first hash values, it errantly attributes such disclosure to *Williams*. With respect, Applicant must point out that *Williams* does not disclose that which the Office attributes to it.

Williams' disclosure is directed to a method by which a device such as a mobile phone may delegate certificate validation to a more capable computational system such as a server. In

describing a typical set of circumstances, the disclosure of *Williams* happens to use terms such as CRL, delta CRL, digital signature and hash value. However, that is the extent of any similarity between *Williams* and the subject matter claimed by Applicant.

Relative to the subject matter claimed, neither *Zhao* nor *Williams* involve the use of hash values computed as a function of a resultant state computable from information conveyed, as compared to a conventional hash of the specific information conveyed. Applicant's claim 3 recites with considerable specificity, a first hash value of this type conveyed together with a delta CRL. Thus, the first hash value is not be computed over the delta CRL, but rather over a resultant state computable after applying the delta CRL to a based CRL state. Claim 3 goes on to recite validation of an update by computing a second hash value from a locally computed resultant CRL state and comparing same to the received first hash value.

To be clear, neither *Zhao* nor *Williams*, taken alone or in combination discloses or suggests a method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, where the method includes:

> receiving a delta coded update to a certificate revocation list **(a delta CRL) together with an associated first hash value,** the delta CRL encoding an update to a preceding certificate revocation list state CRL(t) and the **first hash value computed as a function of at least a resultant state CRL(t+1)** computable by applying the delta CRL to the CRL(t) state;
>
> computing an update to a local certificate revocation list state by applying the received delta CRL to produce a resultant local CRL state; and
>
> validating the update at least in part by computing a **second hash value as a function of at least the resultant local CRL state** and comparing the second and first hash values.

In fact, the Office's bold assertion to the contrary (*see* Office action, pages 5-6) is, at best, mistaken. The Office's statements have no basis in fact. As a result, they cannot and do not create a *prima facie* case of obviousness. Simply stated, a sustainable rejection under § 103 requires more than just random usage of the two terms, "CRL" and "hash." The present rejection is not sustainable and Applicant respectfully requests that it be withdrawn. Claim 3 and those dependent therefrom (claims 4-10 and 19-20) are all allowable for at least the foregoing reason(s).

Of note, claim 5 adds the further limitation that first and second hash values are computed over both prior and resultant states (i.e., CRL(t) and CRL(t+1)). Claim 7 is similar, though of differing scope. In both cases, and as before, the specific subject matter claimed is neither disclosed nor suggested by *Zhao* or *Williams*, whether taken alone or in combination. Again, the Office's bold assertions to the contrary (*see* Office action, pages 7, 9) have no factual basis in the actual disclosure of *Williams*. These rejections are likewise unsustainable and Applicant respectfully requests that each be withdrawn.

Independent claims 11, 16 and 21 are each of differing scope; nonetheless, each is allowable over the applied art for at least reasons analogous to those presented above with respect to claim 3. As before, the Office's rejections of claims 11, 16 and 21 are not supported by any plausible interpretation of the actual disclosure of *Williams*. As before, disclosure attributed to *Williams* simply does not appear therein and the Office's rejections lack a sustainable evidentiary basis.

Objections to the Specification

Finally, the Office makes several objections to the specification ostensibly under 37 CFR 1.75(d)(1), based on absence of definitions for the terms "computer program product" and "computer readable encoding." In particular, the Office suggests that it is unable to ascertain the meaning of constituent terms "program" and "product" and "readable." With respect, the Office is encouraged to consult any of a variety of English language dictionaries. In addition, Applicant respectfully points out that the phrase "computer program product" appears in over 27,000 issued US patents, while the precise phrase "computer readable encoding" appears in 33 issued US patents.

If the Office persists in its requirement, Applicant will make an appropriate amendment to the description to provide clear antecedent basis for the terms. However, particularly in view of the routine use of similar terminology in various issued US patents, Applicant respectfully requests that the Office reconsider and withdraw its objections.

Conclusion

In summary, claims 3-23 are in the case. All claims are believed to be allowable over the art of record, and a Notice of Allowance to that effect is respectfully solicited. Nonetheless, if any issues remain that could be more efficiently handled by telephone, the Examiner is requested to call the undersigned at the number listed below.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

/David W. O'Brien, signed 29-Sep-08/ Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

/David W. O'Brien/

David W. O'Brien, Reg. No. 40,107
Attorney for Applicant(s)
(512) 338-6314 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)